

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH
614-377-4009 THAT IS STORED AT PREMISES
CONTROLLED BY T-MOBILE US, INC.

Case No.

1:19MJ-487

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

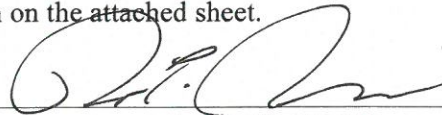
18 U.S.C. 1503

Obstruction of the Due Administration of Justice

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

DUSM, Nathan Richardson, U.S. Marshals Service

Printed name and title

Sworn to before me and signed in my presence.

Date:

6/27/19

Judge's signature

City and state: Cincinnati, Ohio

Hon. Karen L. Litkovitz, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **614-377-4009** that is stored at premises owned, maintained, controlled, or operated by T-Mobile US, Inc., a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by T-Mobile US, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of T-Mobile US, Inc., , regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to T-Mobile US, Inc. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), T-Mobile US, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages from **July 2018 to date of this order** stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from **July 2018 to date of this order**;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message from **July 2018 to date of this order**;

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from **July 2018 to date of this order;**

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from **July 2018 to date of this order;**

h. Incoming and outgoing telephone numbers, from **July 2018 to date of this order;**

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between T-Mobile US, Inc. and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1503 involving Teela GILBERT and Barry Renee Isaacs since **July 2018**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence of communications concerning the IRS and grand jury investigations;
- b. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- c. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- d. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- e. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- f. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to obstruction or tax offenses, including records that help reveal their whereabouts.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
614-377-4009 THAT IS STORED AT
PREMISES CONTROLLED BY
T-MOBILE US, INC.

Case No. **1:19MJ-487**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Deputy United States Marshal (DUSM) Nathan Richardson, being first duly sworn,
hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by T-Mobile US, Inc., a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require T-Mobile US, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a law enforcement officer with the United States Marshals Service and have been since 2016. I am currently assigned as a DUSM /Team Leader to the Fugitive Task Force of the United States Marshals Service and have been so assigned since July 2018. In connection with

my official duties, I am involved in investigations relating to violations of federal statutes, including, 18 U.S.C. § 1503, Obstruction of the Due Administration of Justice.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1503 have been committed by Teela GILBERT. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The United States, including U.S. Marshal’s Service, is conducting a criminal investigation of Berry Rene Isaacs and Teela GILBERT regarding possible violations of 18 U.S.C. 1503.

7. On or about April 10, 2019, Teela GILBERT was indicted for Obstruction of the Due Administration of Justice in violation of 18 U.S.C. §§ 1503 and 2. The indictment alleges that on or about February 6, 2019, GILBERT made material false statements under oath during a federal grand jury investigation in the Southern District of Ohio and further alleges that her co-

defendant Barry Rene Isaacs aided and abetted GILBERT in concealing or withholding documents and making false statements. GILBERT admitted that she had spoken to Isaacs by phone and that he was aware that she would be testifying before the grand jury. Further investigation by the IRS and USMS determined that GILBERT routinely used the phone number **614-377-4009** (the **Subject Telephone 1**) in her communications with law enforcement and others.

8. As set forth herein, probable cause exists to believe that the information specified in Attachment B, which is incorporated herein by reference, including the requested geo-location data from **Subject Telephone 1**, will constitute or lead to evidence of offenses involving obstruction of justice in violation of 18 U.S.C. § 1503. GILBERT is currently considered a fugitive by law enforcement and the requested geo-location data from **Subject Telephone 1** will assist law enforcement in the arrest of GILBERT. For the reasons set forth above, there is also probable cause to believe that obstruction of justice has been committed, are being committed, and will continue to be committed by GILBERT while **Subject Telephone 1** is in her possession.

9. In my training and experience, I have learned that T-Mobile US, Inc. is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for T-Mobile US, Inc. subscribers may be located on the computers of T-Mobile US, Inc. Further, I am aware that computers located at T-Mobile US, Inc. contain information and other stored electronic communications belonging to unrelated third parties.

10. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of T-Mobile US, Inc. for weeks or months.

11. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone

or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as “Short Message Service” (“SMS”) or “Multimedia Messaging Service” (“MMS”), and is often referred to generically as “text messaging.” Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by T-Mobile US, Inc. for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber’s account.

12. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

13. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic

Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

14. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

15. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

16. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

17. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include

both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

18. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require T-Mobile US, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

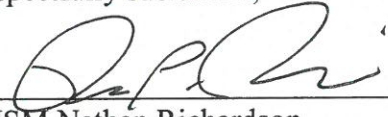
19. Based on the forgoing, I request that the Court issue the proposed search warrant.

REQUEST FOR SEALING

20. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

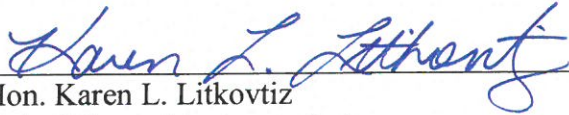
destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Richardson', written over a horizontal line.

DUSM Nathan Richardson
United States Marshals Service

Subscribed and sworn to before me on this 27 day of June 2019

A handwritten signature in blue ink, appearing to read 'Karen L. Litkovtiz', written over a horizontal line.

Hon. Karen L. Litkovtiz
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **614-377-4009** that is stored at premises owned, maintained, controlled, or operated by T-Mobile US, Inc., a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by T-Mobile US, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of T-Mobile US, Inc., , regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to T-Mobile US, Inc. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), T-Mobile US, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages from **July 2018 to date of this order** stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from **July 2018 to date of this order**;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message from **July 2018 to date of this order**;

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from **July 2018 to date of this order;**

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from **July 2018 to date of this order;**

h. Incoming and outgoing telephone numbers, from **July 2018 to date of this order;**

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between T-Mobile US, Inc. and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1503 involving Teela GILBERT and Barry Renee Isaacs since **July 2018**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence of communications concerning the IRS and grand jury investigations;
- b. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- c. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- d. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- e. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- f. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to obstruction or tax offenses, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by T-Mobile US, Inc. and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of T-Mobile US, Inc. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of T-Mobile US, Inc., and they were made by T-Mobile US, Inc. as a regular practice; and

b. such records were generated by T-Mobile US, Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of T-Mobile US, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by T-Mobile US, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature